2018

# Four Principles for Digital Expression (You Won't Believe #3!)

Danielle K. Citron
*Boston University School of Law*

Neil Richards
*Washington University School of Law in St. Louis*

# FOUR PRINCIPLES FOR DIGITAL EXPRESSION (YOU WON'T BELIEVE #3!)

**DANIELLE KEATS CITRON[*] & NEIL M. RICHARDS[**]**

ABSTRACT

*At the dawn of the Internet's emergence, the Supreme Court rhapsodized about its potential as a tool for free expression and political liberation. In ACLU v. Reno (1997), the Supreme Court adopted a bold vision of Internet expression to strike down a federal law - the Communications Decency Act - that restricted digital expression to forms that were merely "decent." Far more than the printing press, the Court explained, the mid-90s Internet enabled anyone to become a town crier. Communication no longer required the permission of powerful entities. With a network connection, the powerless had as much luck reaching a mass audience as the powerful. The "special justifications or regulation of the broadcast media" had no application to the "vast democratic forums of the Internet."*

*Twenty years later, the Roberts Court had an opportunity to explain how the First Amendment should operate in the mature Internet of 2017. Despite the interval of time, the Roberts Court of 2017 took a remarkably similar approach to the Rehnquist Court of 1997. In Packingham v. North Carolina, Justice Kennedy announced the start of the "Cyber Age." The Internet was the virtual public square, much like streets and parks. Because the "Internet" was still in its infancy, its impact on expression was not fully understood. The expressive potential of the "Internet" would be imperiled in the absence of a hands-off approach. Justice Kennedy noted that someday, the Internet might be used for anti-social ends. Until then, extreme caution was in order so the Internet's democratic potential could be realized.*

---

[*] Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law; Affiliate Fellow, Yale Information Society Project; Affiliate Scholar, Stanford Center on Internet & Society.

[**] Thomas & Karole Green Professor of Law, Washington University; Affiliate Fellow, Yale Information Society Project; Affiliate Scholar, Stanford Center on Internet & Society. We would like to thank our deans, Nancy Staudt, Donald Tobin, Rebecca Hollander-Blumoff, and Mike Pappas, as well as Greg Magarian and the participants in and editors of the *Washington University Law Review*'s symposium on his book, *Managed Speech: The Roberts Court's First Amendment* (2017). We would especially like to thank our commentators, Lee Epstein and Michael Kahn.

*Contrary to the Court's thinking, the Internet is no longer in its infancy. It has matured at a breathtaking pace. Virtually all aspects of our public and private lives - politics, child-rearing, work, health, shopping, and sex - involve the Internet. If online discourse ever accorded with the Court's vision, it does not now. Rather than just the virtual town square, the "Internet" is bound up in everything and everywhere-whether the workplace, library, coffee shop, gym, park, public street, town square, or bedroom.*

*This article debunks the Court's magical thinking about the Internet. The Internet's expressive opportunities are not available to all on equal terms, thanks to the wide availability of personal data. Online platforms highlight favored content while burying disfavored ones. Search engines produce different, and less advantageous, results to people of color and women than to men. Cyber mobs shove people offline with doxxing, swatting, and other privacy-invasive forms of abuse. Online platforms fuel polarization and filter bubbles, ensuring an electorate without access to a full range of ideas and information. Fake news spreads like wildfire on social media platforms that are often people's main source of information.*

*We need clear principles to guide and secure meaningful digital free expression. This article charts a path to provide just that. Part I exposes crucial myths surrounding the digital speech and privacy in our networked age. Part II offers a conception of free speech based on a distrust of power, both public and private. Even if doctrinal analysis does not account for private barriers to free expression, the project of free expression should. Part III lays out four essential preconditions for a theory and a system of free expression in the digital age. These preconditions are substantive and procedural. They require legal intervention and extra-legal efforts. They draw some inspiration from due process guarantees and some from commitments to equality. Underlying these principles is a unifying normative commitment: If we want to ensure that our commitment to long-standing democratic theories of free expression survives its translation to the digital environment, we need to take a long, hard look at the digital public sphere we actually have, rather than one that we might want or one that has been advertised to us by Silicon Valley.*

## INTRODUCTION

At the dawn of the Internet's public emergence, the Supreme Court rhapsodized about its potential for free expression and political liberation. In *Reno v. ACLU*,[1] the Supreme Court adopted a bold vision of Internet expression in striking down a federal law—the Communications Decency Act—that would have limited digital expression to forms that were merely "decent." Far more than the printing press, the Court explained, the mid-'90s Internet of web pages and chat rooms enabled anyone to become a virtual town crier. Speakers no longer needed the permission of powerful media companies to reach the public, because the Internet levelled the playing field between powerless speakers and powerful printers or broadcasters. Unlike mass media that controlled what content would reach people in their homes, the Internet enabled all manner of speakers and expression to reach the public at large assuming they had a computer, a modem and a phone line. As a result, the Court held that the "special justifications for regulation of the broadcast media" had no application to the "vast democratic forums of the Internet."[2]

Exactly twenty years later, the Roberts Court had an opportunity to explain how the First Amendment should operate in the face of a mature Internet. Despite the lapse of time, and the massive technological shifts to broadband, social media, and ubiquitous smartphones, the Roberts Court of 2017 took a remarkably similar approach to the Rehnquist Court of 1997. In *Packingham v. North Carolina*,[3] Justice Kennedy announced the start of the "Cyber Age," featuring the Internet as the "modern public square." Because the Internet was still in its infancy, he suggested, its impact on expression could not be fully understood. Law could imperil the Internet's expressive potential. Someday, the Internet *might* be used for antisocial ends, Justice Kennedy noted, but until then, extreme caution was necessary to protect the Internet's democratic potential.[4]

Contrary to the Court's thinking, the Internet is not a babe in the woods. Nor is it separate from everyday life. Today, virtually *all* aspects of our public and private lives—politics, child-rearing, work, health, shopping, and sex—involve the Internet. If online discourse ever accorded with the Court's vision, it certainly does not now. Social interaction, intellectual exploration, political and cultural engagement, employment, and all other manner of life's projects involve networked technologies. Rather than just

1. 521 U.S. 844 (1997).
2. *Id.* at 868.
3. 137 S. Ct. 1730 (2017).
4. *Id.* at 1737.

the virtual town square, the Internet is bound up in everything we do and everywhere we do it—whether in the workplace, library, coffee shop, gym, park, street, or old-fashioned town square.

Meanwhile, the Internet's indispensability is paired with its inequality of control and opportunity. Private owners of Internet infrastructure, from content layer to backbone, block, filter, mute, and decrease the visibility of online expression, making it difficult for some to engage in public discourse. Not only do companies determine *who* participates, but they control *what* content is available and to *whom*. Online service providers and search engines tailor people's online experiences based on fine-grained surveillance about their past communications, interactions, and activities. When searching for "financial news," for example, African Americans may see stories on payday loans while whites may see links for low-interest mortgages. People over forty may not see advertisements for employment, thanks to algorithms facilitating Facebook Ads.[5] While government censorship remains a danger, communication and participation in the digital age are imperiled by private power as well as that of the state.

This essay takes a critical look at the theory of the Internet and expression implicit in *Reno* and *Packingham*. In so doing, it seeks to debunk some of the Court's magical thinking about the Internet. Contrary to the Court's assumptions, the Internet's expressive opportunities are not available to all on equal terms. Everyone cannot be a virtual town crier as the Court imagined. Private entities serve as powerful gatekeepers to digital expression. The design of our digital infrastructure can preclude people from accessing online platforms.[6] Platforms highlight favored content while burying or blocking disfavored ones (more often unpopular speakers). Search engines produce different, and less advantageous, results to the vulnerable than to the powerful.[7] Cyber mobs shove people offline with doxxing, swatting, and other privacy-invasive forms of abuse.[8] Fake news

5. Julia Angwin, Ariana Tobin & Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, PROPUBLICA (Nov. 21, 2017, 1:23 PM), https://www.propublica.org/article/ facebook-advertising- discrimination-housing-race-sex-national-origin.

6. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).

7. LaTanya Sweeney, *Discrimination in Online Ad Delivery*, COMM. ACM, May 2013, at 44, 45; Sonia Katyal, *Algorithmic Civil Rights*, 103 IOWA L. REV. (forthcoming 2018) (on file with author) (discussing study where women disproportionately see ads for less well-paying jobs than men searching same terms).

8. *See generally* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014) [hereinafter CITRON, HATE CRIMES]; Danielle Keats Citron, *Online Engagement on Equal Terms*, B.U. L. REV. ONLINE (Oct. 19, 2015), https://www.bu.edu/bulawreview/bulronline/citron-online-engagement-on-equal-terms/; Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009); Danielle Keats Citron, *Yale ISP—Reputation Economies in Cyberspace Part 3*, YOUTUBE (Dec. 8, 2007), https://www.youtube.com/watch?v=XVEL4RfN3uQ.

spreads like wildfire on social media sites, which may be people's main source of information.[9] Internet service providers surveil our online activities, sharing them with online advertisers who tailor the content made visible to us.[10]

Although these massive corporations—whether they call themselves "social media," "tech companies," or "neutral platforms"—hold most of the cards, the First Amendment has almost no application to their policies. The central battleground for free speech and privacy will be fought in corporate boardrooms rather than in the courts. The most important legal instruments governing free speech on the Internet today are not derived from the Constitution, but from contract law—the terms of service governing the relationship between Internet companies and their customers.

Our argument proceeds in three steps. Part I exposes crucial myths surrounding digital speech and privacy in our networked age. Part II offers a conception of free speech based on a distrust of power, both public and private. Even if constitutional doctrine does not account for private barriers to free expression, we argue, the project of free expression must. Part III lays out four essential preconditions for a theory and a system of free expression in the digital age.

Let us be clear at the outset: We remain committed to robust free expression and to the spirit of *New York Times v. Sullivan*.[11] We believe that the outcomes in *Reno* and *Packingham* are correct. The First Amendment does and should prohibit the state from reducing digital expression to that which is "decent" and fit for children; the First Amendment does and should prohibit the state from indiscriminately barring felons (or anyone else) from the Internet. But theory matters. And good theories should bear a close relationship to the messy reality we live in rather than to utopian visions that ignore obvious power dynamics. Underlying our four principles is a unifying normative commitment to ensuring that our traditional free speech values survive the translation to the digital environment. That will require taking a long, hard look at the digital public sphere that we actually have, rather than one we might want to have or that Silicon Valley has tried to sell to us.

---

9. *See generally* Robert Chesney & Danielle Citron, *Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?*, LAWFARE (Feb. 21, 2018), https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy.

10. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015) [hereinafter RICHARDS, INTELLECTUAL PRIVACY]; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689 (2013).

11. 376 U.S. 254 (1964). *See also* CITRON, HATE CRIMES, *supra* note 8; RICHARDS, INTELLECTUAL PRIVACY, *supra* note 10.

## I. THE REALITIES OF DIGITAL EXPRESSION

For twenty years, the Supreme Court has remained steadfast in its characterization of the Internet as a virtual "public square" that enables anyone to become a "town crier."[12] That vision overlooks crucial realities confronting speakers and audiences in the digital age. Jurisprudential folly, misguided policy, and injustice can result from such misunderstandings. The Court needs a Brandeis brief on the lived realities of digital expression, which this part supplies.

### *A. The Idealized Internet*

In *Reno v. ACLU*, decided in 1997, the Court described the Internet as constituting "vast democratic forums."[13] At issue in *Reno* were provisions of the Communications Decency Act of 1996 (CDA) that criminalized the "knowing" transmission of "obscene or indecent" messages to underage recipients, or "knowingly" sending or displaying to a minor any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."[14] In essence, the law was an attempt to ensure that content on the Internet was "decent" and fit for children.

The Supreme Court struck down those provisions of the CDA as unconstitutionally vague.[15] Justice Stevens, writing for the Court, held that the law impermissibly risked limiting adults' access to material, such as literature, that included content the state might deem "indecent."[16] For the Court, Internet expression was too important to be limited only to what government officials think is fit for children.[17]

The Court underscored that unlike mass media that concentrated power over expression in the hands of the few, the Internet distributed power over expression to the many.[18] The Court characterized the Internet in this way: "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer."[19] The special justifications for the regulation of content decency in broadcast media thus had no

12. Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017); Reno v. ACLU, 521 U.S. 844, 870 (1997).
13. 521 U.S. at 868.
14. *Id.* at 859–60.
15. *Id.* at 874.
16. *Id.*
17. *Id.* at 875.
18. *Id.* at 870.
19. *Id.*

application to the Internet.[20] The Internet should be treated as a newspaper rather than a television station broadcasting over a scarce resource.[21]

Twenty years later, the Court in *Packingham v. North Carolina* struck a similar chord.[22] This time, the issue was the constitutionality of a state law prohibiting registered sex offenders from accessing social network sites used by minors.[23] The Court talked about the Internet as if little had changed in twenty years. Justice Kennedy, writing for the majority, declared that "cyberspace" was a "quintessential forum for the exercise of First Amendment rights" much like a public street or park.[24] Social media sites were hailed as special zones of public discourse.[25] According to the majority, social networks "provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard."[26] Social media "allows users to gain access to information and communicate with one another about it on any subject that might come to mind."[27] As the Court observed, on social media platforms like Facebook, LinkedIn, and Twitter, individuals can debate religion and politics, look for employment, and petition government representatives.[28]

The Court struck down the North Carolina law because it burdened substantially more speech than was necessary to further the government's legitimate interest in protecting minors from registered sex offenders.[29] The government's interest could not justify a prohibition that operated as a "complete bar to the exercise of First Amendment rights on websites integral to the fabric of our modern society and culture."[30] As a result, the statute was facially unconstitutional because it excluded sex offenders from the "modern public square."[31]

### *B. From Myth to Reality*

Today's Internet is not the virtual town square mythologized by the Court. Although the Internet enables interaction, creativity, discussion, persuasion, and access to knowledge, it enables far more than public

20. *Id.*
21. *Id.*
22. 137 S. Ct. 1730 (2017).
23. *Id.* at 1733–34.
24. *Id.* at 1735.
25. *Id.*
26. *Id.* at 1737.
27. *Id.*
28. *Id.* at 1735.
29. *Id.* at 1738.
30. *Id.*
31. *Id.*

discourse.[32] Online platforms host a dizzying array of activities, from work and play to commercial activities and group associations.[33] Some sites and profiles are de facto workplaces. Some establish professional bona fides necessary to attract clients and business. Some operate as stores with hubs for consumer reviews. Some facilitate illicit activities, such as the purchase of drugs, sex, passwords, and stolen credit card numbers. Some are part of educational institutions or their virtual equivalents. Some are password protected; others are accessible to all comers.[34]

Beyond its one-dimensional view of the Internet as a virtual town square, the Court makes other important errors about digital expression. As this section explores, digital expressive opportunities are neither limitless nor uniform. This results from several factors, including the private nature of our digital infrastructure; the censorial power of companies (at times exerted at the behest of non-U.S. nations); the silencing impact of cyber mobs, stalkers, and trolls; and distinct pathologies of our networked environment.

### *1. The Nature of the "Public Square"*

At the risk of stating the obvious, the defining hallmark of the "public square" is that it is *public*. This is true in at least two important senses of the word. First, the public square is "public" in the sense that it is *owned* by the public.[35] Think, in this respect, of "public schools" or the "public sector," Owned by the people for (at least in theory) the benefit of all Second, a public square is "public" in the sense that it is *open* to the public.[36] Public parks, streets, and sidewalks are available for public access and use as a matter of constitutional right. The Supreme Court has built the public forum doctrine on the premise that parks, streets, and sidewalks have been open for speech "immemorially . . . time out of mind."[37] Legislatures can place time, place, and manner restrictions on public fora; they can even close them.[38] But they cannot restrict access to them based on the content of speech or the viewpoint of speakers.

32. *See* CITRON, HATE CRIMES, *supra* note 8. We use the term public discourse to mean, as Jack Balkin suggests, "the processes of communication that allow public opinion to serve as the judge of society." Jack M. Balkin, *Cultural Democracy and the First Amendment*, 110 NW. U. L. REV. 1053, 1072 (2016).

33. *See id.*

34. *See supra* note 8.

35. GREGORY MAGARIAN, MANAGED SPEECH: THE ROBERTS COURT'S FIRST AMENDMENT 100 (2017).

36. *Id.* at 101.

37. Hague v. Comm. for Indus. Org., 307 U.S. 496, 515 (1939).

38. *Cf.* Commonwealth v. Davis, 39 N.E. 113, 113 (Mass. 1895), *aff'd*, Davis v. Massachusetts, 167 U.S. 43, 47 (1897).

The Internet is substantially different from the public square along these dimensions of ownership and openness. The Internet, as experienced by most users, is not publicly-owned. Private companies oversee the digital infrastructure, commonly thought of as a series of layers or stacks.[39] At the risk of oversimplifying, the layers of the Internet are envisioned as ranging from *content* that can be read or interacted with at the top layer, transmission *protocols* in the middle layer, and physical *infrastructure* on the bottom layer. At the top layer, platforms publish content, enabling the posting and consumption of words, images, and videos.[40] Search engines connect individuals with content.[41] Browsers organize content into consumable form.[42] In the middle layer, hosts provide the protocols which platforms require to function.[43] Transit providers connect hosts to the Internet.[44] Security providers ensure that content loads quickly and is protected from attack. At the bottom layer, Internet service and broadband providers handle the flow of data over the network. Throughout, payment systems make it possible to fund online enterprises.[45]

What is notable about this account of the Internet's structure is that, at every layer of the stack, virtually all of the Internet is privately-owned. Private companies control access to the Internet. There are some exceptions. Government entities participate in the Internet Corporation for Assigned Names and Numbers (ICANN), the organization that sets the rules for domain name registrars and registries; provide content on the web at .gov domains; and occasionally serve as Internet Service Providers.[46] But, in the main, private entities are the Internet's gatekeepers, determining who gets access and what online services, platforms, and applications can be viewed, accessed, and consumed.

### *2. Digital Gatekeepers & Nation-State Minders*

Online spaces—the Internet—are not limitless zones of expression. In fact, they may be more limited than offline spaces. In practice, the

39. *See* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815 (2004).

40. Matthew Prince, *Why We Terminated Daily Stormer*, CLOUDFLARE BLOG (Aug. 16, 2017), https://perma.cc/7NB7-LJGJ.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

45. Jack M. Balkin, *Free Speech in an Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS. L. REV. 1149, 1174 (2018).

46. Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1, 23 (2007).

permissibility and visibility of digital speech depends upon companies' speech policies and practices.[47] What a person says and reads online depends upon the decisions of digital infrastructure providers.[48]

At the top layer, content platforms exert significant control over digital expression.[49] In her exhaustive survey of the censorial powers of social media providers, Kate Klonick has aptly described them as the "new speech governors" due to the power that they wield over users' expression.[50] Platforms have speech rules in terms-of-service (TOS) agreements and community guidelines. TOS agreements commonly prohibit child pornography, phishing, spam, fraud, copyright violations, impersonation, hate speech, nonconsensual pornography, violent extremism, and threats.[51] Typically, platforms rely on users to report TOS violations. With the help of moderators[52] with varying degrees of review, platforms determine if the reported content (and sometimes the speaker) can remain online.

Beyond the operation of speech policies in TOS agreements, companies use machine-learning algorithms to prioritize, obscure, or block expression before it ever appears.[53] On Facebook's News Feed, some content is highlighted while other content is hidden or blocked. Facebook employs algorithms to detect and remove terrorist speech.[54] YouTube employs a tool called Content ID to prevent copyrighted material from being posted without the author's consent.[55] The dominant online platforms—Twitter, Facebook, Microsoft, and YouTube—are developing an industry database

47. *See* Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age*, 91 B.U. L. REV. 1435 (2011).

48. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. (forthcoming 2018).

49. CITRON, HATE CRIMES, *supra* note 6, at 168.

50. Klonick, *supra* note 48.

51. Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035 (2018).

52. The major platforms have thousands of content moderators operationalizing speech rules and practices. Facebook says that by 2018 it will have 20,000 content moderators working on TOS complaints. Anita Balakrishnan, *Facebook Pledges to Double Its 10,000-Person Safety and Security Staff by End of 2018*, CNBC (Oct. 31, 2017, 7:59 PM), https://www.cnbc.com/2017/10/31/facebook-senate-testimony-doubling-security-group-to-20000-in-2018.html.

53. Researchers have found that using algorithms to detect hate speech will result in far more false positives than false negatives because they cannot capture context—tone, speaker, and audience. NATASHA DUARTE ET AL., CTR. FOR DEMOCRACY & TECH., MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 4 (2017), https://perma.cc/B2UE-A26H. Although natural language processing algorithms can be trained to detect various combinations and collections of words, they cannot distinguish jokes, sarcasm, or rebuttals of hate speech from hateful statements. *Id.* at 19. Algorithms also reinforce bias that exists in the training data—that is why they perform less accurately when analyzing the language of female speakers and African American speakers. *Id.* at 15.

54. Sheera Frenkel, *Facebook Will Use Artificial Intelligence to Uncover Extremist Posts*, N.Y. TIMES, June 16, 2017, at B4.

55. Matthew Sag, *Internet Safe Harbors and the Transformation of Copyright Law*, 93 NOTRE DAME L. REV. 499, 538 (2017).

that will collect hashes—or unique digital fingerprints—of banned violent extremist content for instant flagging, review, and removal.[56]

The power to control digital expression extends to all layers of the Internet. Without security protections, it can be impossible to remain online.[57] Cloudflare, for instance, helps protect sites from distributed denial-of-service attacks (DDoS).[58] After the deadly neo-Nazi march in Charlottesville, Virginia, the *Daily Stormer*'s operator, Andrew Anglin, praised the man who drove a car into a crowd of civil rights activists and killed Heather Heyer. Cloudflare CEO Matthew Prince explained that hackers urged the company to "get out of the way" so that they could take the site off the Internet.[59] In the face of public pressure, Cloudflare dropped *Daily Stormer* as a client.[60] Hackers were able to shut down the *Daily Stormer* because it lacked protection from the hackers' DDoS attacks. In a subsequent blog post, Prince expressed regret about having gotten involved with policing content.[61]

Sometimes, market forces are behind companies' retail and wholesale decisions to censor speech.[62] As in Cloudflare's case, companies may be caving to public pressure when they take away a particular speaker's ability to engage online.[63] They may alter their speech policies and practices to attract advertising fees and advocates' approval.[64] For some platforms, combating cyber harassment is key to their bottom line.[65] In May 2013, fifteen companies, including Nissan, threatened to pull their ads on Facebook unless it removed profiles that glorified or trivialized violence against women.[66]

56. Kaveh Waddell, *A Tool to Delete Beheading Videos Before They Even Appear Online*, THE ATLANTIC (June 22, 2016), https://www.theatlantic.com/technology/archive/2016/06/a-tool-to-delete-beheading-videos-before-they-even-appear-online/488105/. Hashing is a "mathematical operation that takes a long stream of data of arbitrary length, like a video clip or string of DNA, and assigns it a specific value of a fixed length, known as a hash. The same files or DNA strings will be given the same hash, allowing computers to quickly and easily spot duplicates." Jamie Condliffe, *Facebook and Google May Be Fighting Terrorist Videos With Algorithms*, MIT TECH. REV. (June 27, 2016), https://perma.cc/DA72-X7RH.

57. That is, anywhere except the Dark Web.

58. Prince, *supra* note 40.

59. *Id.*

60. Steven Johnson, *Why Cloudflare Let an Extremist Stronghold Burn*, WIRED (Jan. 16, 2018, 6:00 AM), https://perma.cc/XZW3-7D2C.

61. Prince, *supra* note 40.

62. Citron, *Extremist Speech*, supra note 51.

63. Johnson, *supra* note 60.

64. CITRON, HATE CRIMES, *supra* note 8, at 229.

65. *Id.*

66. *Id.*

In other instances, companies engage in private censorship to stave off threatened regulation.[67] After terrorist attacks in Paris and Brussels in late 2015, European regulators excoriated tech companies for failing to combat terrorist recruitment on their platforms.[68] Their message was clear: online platforms would face onerous civil and criminal penalties unless their policies and processes resulted in the rapid removal of extremist speech.[69] The major social media companies accommodated EU regulators' demands because regulation of extremist and hateful speech was a real possibility in the European Union.[70]

Payment providers can make it impossible for speakers to remain online. For instance, the sheriff of Cook County, Illinois wrote letters to credit-card companies demanding that they prohibit the use of their cards to purchase advertisements on Backpage.com since ads might be used for illegal sex-related products or services.[71] Backpage responded by seeking a preliminary injunction against the sheriff for violating its First Amendment rights.[72] The court held that the sheriff had irreparably harmed Backpage.com by threatening coercive state action against credit card companies that facilitated payment of advertisements.[73] The court directed the trial court to issue a temporary injunction ordering the sheriff to "take no actions, formal or informal, to coerce or threaten credit card companies, processors, financial institutions, or other third parties with sanctions intended to ban credit card or other financial services from being provided to Backpage.com."[74]

### *3. Cyber Mobs, Stalkers, and Trolls*

In 1997, it would have been difficult to foresee the threat to speech posed by cyber mobs and individual harassers. The Internet was still largely a tool for hobbyists and had not become the essential part of modern life that it occupies today. But now, after ten years of sustained research and public conversation about the phenomena of cyberstalking and harassment, it is

67. Citron, *Extremist Speech*, *supra* note 51. In the United States, threatening to regulate protected speech implicates the protections of the First Amendment. Fairley v. Andrews, 578 F.3d 518, 525 (7th Cir. 2009) ("Threatening penalties for future speech goes by the name 'prior restraint,' and a prior restraint is the quintessential first-amendment violation.").

68. Liat Clark, *Facebook and Twitter Must Tackle Hate Speech or Face New Laws*, WIRED (Dec. 5, 2016), https://perma.cc/3JTT-4DTP.

69. *See* Mark Scott, *Europe Presses U.S. Tech Giants To Curb Online Hate Speech*, N.Y. TIMES, Dec. 7, 2016, at B4; Amar Toor, *UK Lawmakers Say Facebook, Google, and Twitter Are 'Consciously Failing' to Fight ISIS Online*, THE VERGE (Aug. 26, 2016, 5:58 AM), https://perma.cc/HBP4-RZ68.

70. Citron, *Extremist Speech*, *supra* note 51.

71. Backpage.com, LLC v. Dart, 807 F.3d 229, 230 (7th Cir. 2015).

72. *Id.*

73. *Id.* at 238.

74. *Id.* at 239.

undeniable that not everyone can freely engage online.[75] This is especially true for women, minorities, and political dissenters who are more often the targets of cyber mobs and individual harassers. In a connected vein, people who lack the economic means to purchase computers, broadband, and high-end mobile phones cannot participate equally in digital life.

Consider the case of online abuse. Cyberstalking often involves a perfect storm of rape threats, doxxing, nonconsensual pornography (also known as "revenge porn"), and reputation-harming lies.[76] Stalkers impersonate victims on dating sites and call for strangers to rape them. They shut down victims' sites with DDoS attacks.[77] They falsely report victims' profiles as TOS violations in the hopes that their profiles will be suspended or shut down.[78] Cyberstalking victims have difficulty expressing themselves in the face of online assaults.[79] They often withdraw from online activities. They shut down their blogs, sites, and social media profiles not because they tire of them, but because they hope to avoid provoking further abuse. The Electronic Frontier Foundation (EFF) has described cyber harassment as "profoundly damaging to the free speech and privacy rights of the people targeted." EFF recognized the fact that online harassment silences people, especially those with "less political or social power" and "women and racial and religious minorities."[80]

Political dissenters have faced online abuse at the hands of authoritarian regimes. A common strategy of "troll armies" is to drown out political

75. *See*, e.g., CITRON, HATE CRIMES, *supra* note 8, at 35–36; Danielle Keats Citron, *Civil Rights in Our Information Age*, *in* THE OFFENSIVE INTERNET 31, 31 (Saul Levmore & Martha C. Nussbaum eds., 2012); Martha Nussbaum, *Objectification and Internet* Misogyny, *in* THE OFFENSIVE INTERNET 68, 68 (Saul Levmore & Martha C. Nussbaum eds., 2012); Brian Leiter, *Cleaning Cyber-Cesspools: Google and Free Speech*, *in* THE OFFENSIVE INTERNET 155, 155 (Saul Levmore & Martha C. Nussbaum eds., 2012); J. Nathan Matias et. al., *Research: Online Harassment Resource Guide*, WIKIMEDIA (July 3, 2015), https://perma.cc/8FMR-64C7; Nathan Matias, Berkman Fellow, Berkman Klein Luncheon Series at Harvard Law School: Developing Effective Citizen Responses to Discrimination and Harassment Online (Feb. 23, 2016), https://cyber.harvard.edu/events/luncheons/2016/02/Matias; Citron, *Online Engagement on Equal Terms*, *supra* note 8; Neil M. Richards, *The Internet Grows Up?*, B.U. L. REV ONLINE (Nov. 9, 2015), https://www.bu.edu/bulawreview/bulronline/richards-the-internet-grows-up/; Mary Anne Franks, S*exual Harassment 2.0*, 71 MD. L. REV. 655 (2012); Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383 (2009); Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224 (2011); Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, *supra* note 8; Citron, *Cyber Civil Rights*, *supra* note 8.

76. CITRON, HATE CRIMES, *supra* note 8, at 3.

77. *Id.*

78. *Id.*

79. *Id.* at 197.

80. Danny O'Brien & Dia Kayyali, *Facing the Challenge of Online Harassment*, ELECTRONIC FRONTIER FOUND. (Jan. 8, 2015), https://perma.cc/J324-46W8.

expression with spam.[81] Saudi Arabian "cyber troops" flooded Twitter posts critical of the regime with unrelated content and hashtags to obscure the offending post.[82] The Russian government has tried to silence dissenters by spreading falsehoods about them online. Human beings and bots, working on behalf of Russian President Vladimir Putin, relayed the defamatory posts through false accounts on social media sites.[83] During the 2016 election, Russian-paid trolls attacked journalists critical of then presidential candidate Donald J. Trump.[84]

*4. Filter Bubbles, Polarization, and Other Pathologies*

One of the most touted advantages of the modern Internet has been personalization, whether for content, such as "more relevant" advertisements, or for software and devices that adapt to individuals' preferences. Yet personalization has dangers. Almost two decades ago, Cass Sunstein warned that a personalized Internet risked creating a "Daily Me:" an informational monoculture that reflected each individual's personal interests and biases while providing no information to disrupt preconceptions or prejudices. Sunstein was particularly concerned that the "Daily Me" could create destroy our shared democratic culture and the facts upon which democratic society depends and non-personalized twentieth-century mass media had preserved.

Algorithmic filtering can push people's views to extremes. Likes on Facebook can deepen echo chambers, making it more likely that users see posts consistent with their views than those contrary to them.[85] In turn, when groups with similar views get together, their members hear "more and louder echoes of their own voices."[86] As one of us (Citron) has described the phenomenon of group polarization: "Learning that others share their worldviews boosts their confidence. People embrace more radical views

81. Samantha Bradshaw & Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation* 9 (Computational Propaganda Research Project, Working Paper No. 2017.12, 2017), https://perma.cc/K7EX-7JLM.

82. Brian Whitaker, *How Twitter Robots Spam Critics of Saudi Arabia*, AL-BAB (July 28, 2016), https://perma.cc/C6QH-GF5F.

83. *See* TIM WU, KNIGHT FIRST AMENDMENT INST., IS THE FIRST AMENDMENT OBSOLETE? 1, 15 (2017), https://perma.cc/ZWW9-Y55H (describing reverse censorship, flooding and propaganda robots phenomena).

84. David French, *The Price I've Paid for Opposing Donald Trump*, NAT'L REV. (Oct. 21, 2016, 4:55 PM), https://www.nationalreview.com/2016/10/donald-trump-alt-right-Internet-abuse-never-trump-movement/. As French's account illustrated, much of the abuse was imbued with racist and anti-Semitic slurs and images. One of us (Citron) served on the Anti-Defamation League's Task Force on Harassment and Journalism, which issued a report on anti-Semitic targeting of journalists. *See* ANTI-DEFAMATION LEAGUE, ANTI-SEMITIC TARGETING OF JOURNALISTS DURING THE 2016 PRESIDENTIAL CAMPAIGN (2016), https://perma.cc/5JRD-ZY6P.

85. Zeynep Tufekci, *The Real Bias Built in at Facebook*, N.Y. TIMES, May 18, 2016, at A27.

86. CASS R. SUNSTEIN, REPUBLIC.COM 2.0 55 (2007).

because they feel more confident and because they want to be liked. They often exaggerate their views to convince others of their credibility, which leads to [a] sort of competition for persuasiveness . . . ."[87] Hearing supportive voices for online abuse, for instance, encourages more abusive behavior.[88]

Personalization can result in different online experiences based on variables other than politics—in ways that often disadvantage the marginalized. Harvard University Professor Latanya Sweeney found that searches of black-identifying names are twenty-five percent more likely to be served with arrest-related advertisements than searches of white identifying names.[89] The study suggests that there is discrimination in the delivery of advertisements accompanying searches of people's names. Similarly, a study by Carnegie Mellon researchers found that males were more likely to be shown advertisements encouraging the seeking of coaching services for high paying jobs than females.[90] According to the study, there was a statistically significant difference in ads shown to men and women looking for jobs, with men being much more frequently targeted for ads offering high-paying jobs than women were.[91]

## II. POWER AND ITS PRIVATE DISCONTENTS

### *A. Distrust of Power*

There are multiple, overlapping reasons why free speech enjoys exceptional protection under U.S. law, but most of them boil down to power. In one of the most important separate opinions in American law,[92] Justice Louis Brandeis argued in *Whitney v. California* that free speech was worth protecting not for its own sake, but because it safeguarded the social processes of self-governance.[93] In Brandeis' self-governance theory, the act

87. CITRON, HATE CRIMES, *supra* note 8, at 63.
88. *Id.* at 65.
89. Sweeney, *supra* note 7, at 51.
90. Samuel Gibbs, *Women Less Likely to Be Shown Ads for High-Paid Jobs on Google, Study Shows*, THE GUARDIAN (July 8, 2015, 6:29 AM), https://perma.cc/D55G-BQE8.
91. Amit Datta et. al., *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*, 2015 PROC. ON PRIVACY ENHANCING TECH. 92 (2015).
92. Whitney v. California, 274 U.S. 357, 372 (1927) (Brandeis, J., concurring). Justice Brandeis's concurrence has been described as arguably "the most important essay ever written, on or off the bench, on the meaning of the first amendment." PHILLIPA STRUM, SPEAKING FREELY, *WHITNEY V. CALIFORNIA* AND AMERICAN SPEECH LAW 134 (2015) (quoting Vincent Blasi). It has been cited in over 100 Supreme Court opinions and more than 250 opinions in lower federal and state courts. *Id.*
93. *Whitney*, 274 U.S. at 377. *See* Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1323 (2010); G. Edward White, *The First Amendment Comes of Age: The Emergence of Free Speech in Twentieth-Century America*, 95 MICH. L. REV. 299, 325 (1996).

of engaging in free expression produces not just merely better democratic decisions, but better democratic citizens.[94] Free speech allows individuals to participate in the formation of public opinion.[95] It permits citizens to influence—and see themselves as having influenced—state power.[96]

Brandeis' self-governance theory had a major truth-seeking element: "freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth."[97] More broadly, free speech is crucial for the creation of democratic culture.[98] Free speech lets individuals express their values, emotions, opinions, ideas, art, and knowledge. It permits each and every one of us to participate in the development (and revision) of shared cultural meanings.[99]

Yet at bottom, self-governance theory justifies crucial restraints on power. The right to free speech

> is designed and intended to remove governmental restraints from the area of public discussion . . . in the hope that use of such freedom will ultimately produce a more capable citizenry and more perfect polity and in the belief that no other approach would comport with the premise of individual dignity and choice upon which our political system rests.[100]

As Brandeis put it, the theory of the First Amendment was that:

> [b]elieving in the power of reason as applied through public discussion, [the Framers] eschewed silence coerced by law—the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed. Fear of serious injury cannot alone justify suppression of free speech and assembly. Men feared witches and burnt women. It is the function of speech to free men from the bondage of irrational fears.[101]

94. *Whitney*, 274 U.S. at 375–76; *see also* Vincent Blasi, *The First Amendment and the Ideal of Civic Courage: The Brandeis Opinion in* Whitney v. California, 29 WM. & MARY L. REV. 653, 672–73 (1988).

95. Robert C. Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 601, 604 (1990).

96. ROBERT C. POST, DEMOCRACY, EXPERTISE, AND ACADEMIC FREEDOM: A FIRST AMENDMENT JURISPRUDENCE FOR THE MODERN STATE 34–35 (2012).

97. *Whitney*, 274 U.S. at 375.

98. Balkin, *Free Speech in an Algorithmic Society*, *supra* note 45.

99. Balkin, *Cultural Democracy and the First Amendment*, *supra* note 32, 1055–62.

100. Cohen v. California, 403 U.S. 15, 24 (1971).

101. *Whitney*, 274 U.S. at 375–76.

Concerns about power underlie the other leading theory of free speech that emphasizes its importance to the search for political and social truths.[102] In his dissent in *Abrams v. United States*, Justice Oliver Wendell Holmes explained that special protections for free speech are necessary because of the natural human inclination to silence (by force if necessary) opinions that we dislike.[103] "Persecution for the expression of opinions seems to me," he wrote, "perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition."[104] Holmes offered against this certainty, and power's tendency to sweep away disagreement, a principle of epistemic doubt that has remained a defining hallmark of American First Amendment law. Holmes reasoned that the theory of the Constitution was that while truth is elusive, it is far better to allow others to hear what he called "opinions that we loathe and believe to be fraught with death" than to be deprived of that potential insight into truth, or at least the other side of the argument.[105] As he put it well,

> when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.[106]

Holmes offers this principle of doubt as justification for restraints on the power of the state censor, the entity that would choke off dissent and disagreement through the use of its power.

Other scholars have offered a third justification for free expression protections beyond self-governance and the search for truth – the argument that free speech is indispensable to individual autonomy. The account of free speech explains that people cannot decide for themselves how they want to direct their life projects while under the thumb of the state. The right to free speech is thus designed to restrain power from interfering with individual autonomy and dignity.[107]

102. *See* Abrams v. United States, 250 U.S. 616, 624 (1919) (Holmes, J., dissenting).
103. *Id.*
104. *Id.* at 630.
105. *Id.*
106. *Id.*
107. *See e.g.*, Cohen v. California, 403 U.S. 15, 24 (1971).

Ultimately, protections for free speech reinforce the constitutional values of our polity—democratic politics, culture, truth seeking, and individual self-development. To protect these values, the project of free expression warns against power exercised to limit that expression. As Jack Balkin puts it well, freedom of speech ultimately "concerns power—how to regulate it and hold it accountable."[108] Allowing individuals to participate in self-government thus promotes the discovery of truth and builds a shared culture; and allowing individuals to freely express themselves gives power its legitimacy.[109]

It has undeniably been the power of the state that has commanded the attention of judicial free expression doctrine and theory. Most obviously, this is because the First Amendment typically applies only to governments and not to private actors. More deeply, though, the traditions of First Amendment theory reflect a belief that government cannot be trusted to pick winners and losers in the realm of ideas because it will "tend to act on behalf of the ideological powers that be."[110] Government officials fear challenges to the status quo from dissenters who aim to replace them.[111] Without strong free speech protections, outsiders may be unable to challenge governmental power through the practices of ordinary politics.[112] Judge Easterbrook explained, in *American Booksellers Ass'n v. Hudnut,* that the Constitution "forbids the state to declare one perspective right and silence opponents."[113] Yet as Gregory Magarian insightfully explores in his book *Managed Speech*, one of the trends of the Roberts Court's First Amendment decisions is that they have reinforced state and corporate power at the expense of noisy dissenters challenging the status quo.[114] It is becoming a bad time to be what Brandeis termed a "witch."

Doctrinally, the First Amendment applies to the exercise of state power that threatens free speech values.[115] It covers laws, regulations, common law rules, or any action by a person or entity operating under cover of state law

108. Balkin, *Cultural Democracy and the First Amendment*, *supra* note 32, at 1060.

109. *Id.* at 1071.

110. Frank I. Michelman, *Conceptions of Democracy in American Constitutional Argument: The Case of Pornography Regulation*, 56 TENN. L. REV. 291, 302 (1989).

111. On this score, Gregory Magarian agrees (as do we). *See generally* MAGARIAN, *supra* note 35.

112. *See* Am. Booksellers Ass'n v. Hudnut, 771 F.2d 323 (7th Cir. 1985), *aff'd per curiam*, 475 U.S. 1001 (1986); *see also* Kathleen M. Sullivan, *Free Speech Wars*, 48 SMU L. REV. 203, 203–04 (1994). As Susan Brison has argued, the distrust of government account of free speech—rooted in particular political contexts—is more promising than arguments rooted in deontological concerns. Susan J. Brison, *Speech and Other Acts*, 10 LEGAL THEORY 261, 262 n.6 (2004).

113. *Hudnut*, 771 F.2d at 325.

114. MAGARIAN, *supra* note 35, at ch. 7.

115. Michelman, *supra* note 110, at 305.

or in connection with the state.[116] It extends narrowly beyond the state to private parties that have assumed a traditional state function like running a town (though not when running a shopping mall, prison, or public utility).[117] The Supreme Court has taken a functional approach to state action, looking at the substance of whether state power is being used to direct the content of free speech rather than its timing or manner.[118] Thus, in *New York Times v. Sullivan*, the Court extended the protection of the First Amendment to private-law defamation rules, for fear that government officials could censor their critics indirectly through private litigation rather than directly through criminal sedition prosecutions.[119]

Nevertheless, the state action principle is a traditional constraint on constitutional doctrine, designed to ensure that constitutional law focuses on the problems of state power, such as censorship and political tyranny. American constitutional law has been built up over decades with this constraint and focus in mind, and while it is important to consider the state action doctrine functionally, it would be dangerous to substantially or completely jettison it. An overbroad understanding of state action would limit private efforts to protect free speech. If platforms like Facebook or Twitter were treated as quasi-governmental actors, they could not act as "Good Samaritans" to block the assaults of cyber mobs, as contemplated by the drafters of the Communications Decency Act of 1996.[120] They could not protect against spam, doxxing, or impersonations. There is good in having private platforms wield some bounded power to address online abuse and other activity that imperils free expression.

116. Free speech protections do not hinge on simply categorizing something as speech. Speech is a social phenomenon. Conduct can express ideas just as well as words can. Speech triggers the protection of the First Amendment depending on what is being regulated and why it is subject to regulation. The central question is why we are regulating speech rather than whether something is speech or not. Neil M. Richards & Danielle Citron, *Regulating Revenge Porn Isn't Censorship*, ALJAZEERA AM. (Feb. 11, 2015, 2:00 AM), https://perma.cc/RWT5-ZGDE.

117. *See e.g.*, Marsh v. Alabama, 326 U.S. 501, 507–08 (1946); Lloyd Corp. Ltd. v. Tanner, 407 U.S. 551, 569–70 (1972). *Cf.* DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE, ch. 5 (2009) (arguing that some Internet intermediaries such as ISPs should be treated as functional state actors).

118. *See generally* Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1681 (2009). Frank Michelman explains that, "no constitutional text unambiguously prescribes such a rule." Michelman, *supra* note 110, at 306. Although the Fourteenth Amendment's Due Process and Equal Protection clauses speak of the state as the perpetrator and a person as the sufferer, an argument can be made for judicial balancing of the evils of privately wrought deprivations of liberty against the deprivations of liberty wrought by state regulation designed to avert those privately wrought deprivations. *Id.* at 307.

119. 376 U.S. 254, 279–84 (1964); *see also* Solove & Richards, *supra* note 118, at 1681.

120. See Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 404–06 (2017).

Given the state action doctrine, an enormous amount of important expression lacks constitutional protection against the actions of powerful private entities, such as platforms, employers, and property owners. The owners of digital infrastructure, for example, are free to limit the speech of those over whom they exercise economic, social, or other forms of power. In a world where much of our traditional public gathering places are privately-owned, the opportunities for private censorship and interference with the exchange of ideas are widespread. In practice, censorship is more likely to come from companies controlling our digital infrastructure as from state, local, or federal governments.[121]

Expressive freedom needs protection against private power.[122] But that protection must come from sources other than the direct application of constitutional doctrine. If we are interested in the free exchange of ideas to promote self-governance, truth-seeking, democratic culture, and expressive autonomy, we should care about private speech restrictions. The state action doctrine could be amended to prevent certain kinds of private acts of censorship, but doing so would not fully address the problem of private speech restrictions without radically changing our notion of public and private. For better or worse, the public-private divide is foundational to our modern rights jurisprudence.[123] As Julie Cohen argues, we need to pay "more careful attention to naming and demystifying emerging patterns of legal power and privilege" in our digital age.[124]

Private entities wield power over free speech that can be tantamount to—or in excess of—governmental power. They determine what content is and is not acceptable online. Not all private exercises of censorial power are equal, however. In the face of private censorship, people may have alternative outlets to express themselves. An individual blocked from commenting on *The Atlantic*'s website could express her views on *Wired.com*, or on a blog. A user banned from Facebook could recreate a social network elsewhere, though it would be time consuming and likely incomplete. But infrastructure is different. Without Cloudflare's services, the Daily Stormer was knocked off the Internet.[125] In certain locations, people may have only one broadband provider—being banned from that provider would mean no broadband Internet access at all. Cyber harassment

121. *See* Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 436–38 (2009).

122. Michelman, *supra* note 110, at 304.

123. Solove & Richards, *supra* note 118, at 1680–82.

124. Julie E. Cohen, *The Zombie First Amendment*, 56 WM. & MARY L. REV. 1119, 1157 (2015).

125. *See generally* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. U. L. REV. 986 (2008); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

victims often find themselves with no choice but to retreat entirely from online engagement.[126]

Then too, a private entity's amassing of personal data is another way power is exerted over speakers and readers. Uber's God View, which had the capacity to be used to monitor and harass investigative journalists, demonstrated the power that digital technologies can have over the press.[127] Platforms, search engines, broadband providers, and Internet service providers have varying degrees of access to, and control over, what we read, hear, and say online.

Another way to think about censorial private platforms is to consider the First Amendment's recognition of the press as a democratizing institution. That is not to suggest that platforms like Twitter or Facebook amount to the press descriptively or normatively, though the Supreme Court suggested so in *Reno v. ACLU*.[128] Instead, it is to recognize the importance of infrastructures of speech and their importance to democracy and public trust more generally.

There are other ways besides constitutional doctrine to protect free speech and expression. Legal protection for free expression need not take the dramatic form of judges declaring statutes or common law claims unconstitutional. Although such actions are probably necessary in extraordinary cases, they are not the ordinary way that law nurtures and defends our abilities to think and speak as we wish. Law can act away from the limelight of the Constitution and work to protect free expression in less dramatic, more subtle ways as well.

Although largely overlooked in American legal culture, statutes and the common law can safeguard the ability to think, speak, and write freely. These legal tools are far older than our constitutional doctrine of free speech and represent an important way of protecting free expression in a number of important areas where constitutional doctrine is inapposite or ineffective. Our focus on the very successful project of First Amendment law has left these other tools in its shadow, largely forgotten and ignored. This is unfortunate, because these tools are arguably even more important than the doctrinal First Amendment in protecting freedom of speech.

---

126. This has been particularly true for people who lack the resources to hire bodyguards and reputation services. We saw this difference in the online abuse of Yale law students, who lacked a supportive online community and shut down all social media profiles including Facebook and LinkedIn, and feminist journalist and law student Jill Filipovic, who stayed online with the help of thousands of supportive readers who engaged in a Google bomb to ensure that her work remained prominent in search of her name rather than destructive posts of the cyber mob. CITRON, HATE CRIMES, supra note 8, at 69–72.

127. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 782 (2016).

128. 521 U.S. 844 (1997).

Non-constitutional protection of expressive liberties can take at least three forms. At the most basic level, law helps to create the "expressive infrastructure" which makes a robust culture of free expression possible. Free expression is enabled by laws allowing for cheaper rates for newspapers, mandating common carrier rules for companies involved in the dissemination of speech like telephone and Internet companies, and public education at all levels including universities.[129] Common law and statutes can be used to create parallel protections for free expression, such as the long-standing common law doctrine against prior restraints, or copyright's idea/expression distinction and fair use doctrine.

Where constitutional law is under-protective, common law and statutes can fill the gap by creating exemptions or other additional protections for expression. A good example of this gap-filling function is the widespread passage of press shield laws following *Branzburg v. Hayes*, which declined to create a constitutional rule protecting the anonymity of confidential news sources.[130] Another example is Anti-SLAPP laws protecting against lawsuits brought to stifle speech.

Finally, common law and statutes can be used to directly enable free expression through the creation of affirmative rights to speak, unlike constitutional doctrine, which is poorly suited to the creation of affirmative rights due to a number of doctrinal, separation of powers, and cultural limitations. First Amendment doctrine cannot mandate the creation or, alternatively, stop the elimination of parks and other public fora for speech. It merely forbids government discrimination among speakers based upon the content or viewpoint of their message. A government that dislikes the messages emanating from a particular forum is barred by the doctrinal First Amendment from discriminating against those messages but would not be barred from closing the forum entirely. By contrast, positive law can create, fund, and preserve these fora, creating affirmative entitlements to speak.

These are merely a few illustrations of the use of non-constitutional rules to promote free expression. But unlike in the context of state power, we lack the same conceptual and moral vocabulary to talk about excesses of private power. A first step in this process, as we try to ensure the faithful translation of our expressive values to the digital age, is to recognize the need to develop principles to guide the deployment of legal rules to enable, nurture, and protect free expression against the excesses of powerful private and public actors. The following section advances four such principles.

129. *See, e.g.*, Jerome A. Barron, *Access to the Press—A New First Amendment Right*, 80 HARV. L. REV. 1641 (1967); Stephen M. Feldman, *Postmodern Free Expression: A Philosophical Rationale for the Digital Age*, 100 MARQ. L. REV. 1123 (2017).

130. 408 U.S. 665 (1972).

## III. ESSENTIAL PRECONDITIONS FOR DIGITAL EXPRESSION

### *A. Avoiding Magical Thinking*

Like many revolutions, the information revolution unleashed by the mass adoption of networked technologies has its evangelists and its myths. Early Internet evangelists tended to emphasize the radical potential for the Internet to liberate human beings. More recent evangelists have emphasized Silicon Valley's "disruptive innovation," its capacity to continually replace old business models with new ones. Implicit is the belief that disruption is either intrinsically a good thing or that "innovation" tends to produce new good things rather than new bad ones.[131]

However, in the two decades since the Internet's adoption, our lived experience has not fulfilled these revolutionary promises. Digital technologies certainly have the capacity for revolutionary liberation, but they can just as easily be used for oppression. Authoritarian regimes have embraced digital technologies to monitor, surveil, and oppress their people.[132] Even democratic regimes have eagerly used digital technologies for widespread surveillance.[133] The Snowden revelations kick-started a conversation about government surveillance that continues over five years later.[134] Government surveillance has been made far easier in the democratic West by the surveillance-based advertising model upon which "free" services like Google and Facebook have made their vast fortunes.[135]

The Internet of the late 1990s was largely a zone of intellectual privacy; one in which Internet users (or "netizens," to use the now abandoned phrase they used for themselves) could explore niche and unpopular interests free from surveillance. But as corporations realized that the Internet offered vast commercial opportunities, and as Congress repeatedly failed to pass baseline Internet privacy legislation, a surveillance-based advertising industry ascended. Eager to serve better targeted and "more relevant" advertisements, the commercial Internet has become the most surveilled zone of human activity in history. Even if one were to accept the debatable premise that surveillance-based advertising is a necessary evil to promote commerce, the prevalence of state and corporate surveillance in our digital

131. "Disruptive innovation," a term first introduced by Harvard Business School professor Clay Christensen in 1995, has been adopted as a mantra by Silicon Valley about how best to do business in the digital age, somewhat to Christensen's dismay. *See* Clayton Christensen et al., *What Is Disruptive Innovation?*, HARV. BUS. REV., Dec. 2015, at 44.

132. EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 82 (2012).

133. Richards, *The Dangers of Surveillance*, *supra* note 10, at 1938.

134. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014).

135 Id.

age undercuts the promises of revolutionary human liberation that heralded the mass public adoption of the World Wide Web twenty years ago.

Disruptive innovation has a similarly mixed track record with regard to the Internet's claimed promises of liberation. Over the past twenty years, technology companies have innovated and disrupted existing business models, ushering in unprecedented access to information and unprecedented means of low-cost communication. Yet disruptive innovation has imposed a heavy price. Google's search engine may have enabled easy access to information to anyone with an Internet-connected smart phone or laptop, but Google's business model of targeted advertisements has eviscerated the advertising upon which newspapers have depended for decades.[136] While we can now easily look up when the new season of *Game of Thrones* will be available for streaming, newspapers have been forced to drastically reduce the size of their newsrooms and the quality and depth of their reporting.[137] At the same time, digital diversions—whether streaming videos, cute pictures of cats, or the advertisements that fund them—may have made it more difficult to engage in the kind of sustained reading and critical thinking upon which a vital democracy depends. In his book *The Shallows*, Nicholas Carr offers substantial evidence that the skills our malleable brains need to navigate the connected, hyper-linked, short-attention-span digital world may come at the cost of a diminution of our capacity for long, sustained thinking and reading.[138]

Then there are the problems that social media companies have caused with their disruptive innovation. Beyond Facebook's advertising success (which, like Google, has undermined the revenue model of the free press), the social media giant has recently come under sustained criticism for its spreading of filter bubbles, allowing foreign money to influence the most recent presidential election, and failing to stop the spread of "fake news."[139] Twitter, on the other hand, has faced lawsuits by abusive individuals like Charles Johnson alleging that the company's suspension of their accounts violates free speech rights under the California Constitution.[140] At the same time, Twitter has been forced to defend its failure to discipline public figure users like President Donald Trump, who has insulted and threatened foreign and domestic enemies, including threatening North Korea with nuclear

136. FRANKLIN FOER, WORLD WITHOUT MIND: THE EXISTENTIAL THREAT OF BIG TECH 145 (2017).

137. *Id.*

138. NICHOLAS CARR, THE SHALLOWS: WHAT THE INTERNET IS DOING TO OUR BRAINS 119 (2010).

139. Alexis C. Madrigal, *What Facebook Did to American Democracy*, THE ATLANTIC (Oct. 12, 2017), https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/.

140. Issie Lapowsky, *Chuck Johnson's Twitter Free Speech Suit is Probably DOA*, WIRED (Jan. 11, 2018, 12:06 PM), https://www.wired.com/story/chuck-johnson-twitter-free-speech-lawsuit/.

attack, who has targeted private individuals with all manner of abuse, and who has mounted attacks on a free press as "enemies" of the people.[141]

Our purpose in this analysis is not to demonize the Internet, or the technology companies that have made vast fortunes through innovative tools. Our purpose is more modest, which is to suggest that the Internet is a human creation, and that like all human creations, it has complexities that cannot be reduced to platitudes like those offered by tech liberation theories of the 1990s or disruptive innovation theories of the 2000s. Recognizing this fact suggests that in designing policies to ensure meaningful digital expression, we must *avoid magical thinking* of the sort that frequently enters into technology policy debates. We must make policy for the Internet and society that we actually have, not the Internet and society that we might want, or that we believed we would get twenty years ago.

Crucial to the protection of digital speech is to recognize that the Constitution generally and the First Amendment specifically are not the only way to think about our commitment to digital speech. Positive law, social norms, and corporate practices are as important to free speech as constitutional doctrine. Platforms also reflect the unique cultures and norms of their users.[142] As such, we cannot rely on them, or magical thinking about the utopian power of "disruptive innovation" or the invisible hand of the unregulated market (or the self-interested claims made by corporate marketing departments) to ensure the adequate protection of free expression in our digital society. Fundamentally, when we stop thinking magically, we must focus on questions of access and questions of power.

### *B. Inputs Matter*

If we care about digital expression that is meaningfully and broadly available, then we need to start caring more about inputs. First Amendment doctrine typically focuses only on the value of expression, and the state's impact on that expression. This is an entirely sensible approach for a system of negative rights limited by the state action doctrine and for a system that focuses limited judicial resources on questions over which they have the greatest institutional competence and legitimacy.

But if we care not only about the *First Amendment*, but also about our meaningful ability to engage in *free expression*, then the First Amendment is not enough. The First Amendment is no protection for speakers whose

141. Neil Richards, *Free Speech and the Twitter Presidency*, 2017 U. ILL. L. REV. ONLINE (Apr. 29, 2017), https://illinoislawreview.org/symposium/first-100-days/free-speech-and-the-twitter-presidency/ (written as part of the symposium President Trump's First 100 Days)

142. Tufekci, *supra* note 85.

silence is due to an inability to access the Internet. It is no protection for speakers whose expression occurred on private platforms that blocked, filtered, or muted them. It is no protection for speakers subject to retaliation for daring to engage in expression that met with the disapproval of a cyber mob.

Simply put, inputs matter. If we care about the meaningful ability to engage in free expression, and not just the formal capacity to be free from state censorship, our positive law and social policies need to focus on expressive inputs. Of course, there are many inputs that matter, including education and access to leisure time (and even sufficient nutrition), but we shall focus on three inputs that are critically important to digital expression in the present day—intellectual privacy, protection from harassment, and access to the benefits of technology.

First, law must protect intellectual privacy. A critical foundation for meaningful free speech is the ability to generate new, outlandish, and potentially subversive ideas. First Amendment doctrine is highly protective of speakers' ability to say things that are profane, subversive, blasphemous, and insulting without fear of state coercion, but it has paid relatively little attention to the processes by which speakers come to generate ideas in the first place.[143] In a series of articles and a book, one of us (Richards) has argued that our law should protect the value of "intellectual privacy" — freedom from surveillance or interference as we think, read, speak privately, or otherwise engage in the practice of generating new ideas.[144] Yet government and private surveillance has turned the Internet—once touted by libertarian utopianists as a realm of unmonitored access to pure thought—into the single most surveilled realm of human activity in history. Democratic governments, platforms, and advertisers constantly seek to monitor what we watch, read, and write online, for a variety of purposes ranging from the prevention of crime to the pursuit of the perfectly targeted advertisement. These may at times be useful pursuits, but they are not as important as the enablement of democratic deliberation.[145]

Simply put, when we are watched, we change our behavior, inclining it to the boring, the bland, and the mainstream. Our constantly-monitored Internet is a threat to the development of new political and ideological ideas upon which our commitments to intellectual freedom and democratic self-

143. *See* RICHARDS, INTELLECTUAL PRIVACY, *supra* note 10.

144. *See, e.g.*, *id.*; Richards, *Dangers of Surveillance*, *supra* note 10; Neil M. Richards, *Intellectual Privacy*, 87 TEX L. REV. 387 (2008); Richards, *The Puzzle of Brandeis, Privacy, and Speech*, *supra* note 93; Richards, *The Perils of Social Reading*, *supra* note 10.

145. For a sustained argument along this specific line of analysis, see CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA (2017) (arguing in favor of "democratic deliberation" in favor of consumer empowerment as a value in a democracy).

government depend.[146] In developing laws to regulate commerce and surveillance in the digital age, we should not allow the logic of surveillance that motivates business intelligence and law enforcement to create a data collection environment of perfect surveillance. Environments of untrammeled data collection nudge conformity and stifle, if not extinguish, dissent, eccentricity, and creativity. We need to press back against the inexorable pull of what one of us (Citron) has termed the "data collection imperative."[147]

Second, as one of us (Citron) has argued in a series of articles and a book, law, culture, and technology should be brought to bear against online assaults that drive people offline. Law is crucial to deter, redress, and punish cyber mobs and individual harassers who close off avenues for interaction and expression that the Internet opens for most. A legal agenda would serve an expressive role as well, teaching us that online assaults inflict grave damage to victims' important opportunities and to society at large.

A "cyber civil rights" legal agenda should include tort, criminal, and civil rights law.[148] In theory, victims can sue their attackers for intentional infliction of emotional distress, defamation, and public disclosure of private facts (in case of nude photos posted without consent). In practice, however, these lawsuits are expensive to pursue and many victims lack the resources. In what we hope becomes a trend, pioneering law firms like K&L Gates have devoted pro bono resources to combat online abuse so victims with little means can sue their harassers.[149] Prosecutors should use the tools that they have to investigate and prosecute cyber-stalkers, including threat laws and cyber-stalking laws.[150] Crucially, thirty-eight states and the District of Columbia now criminalize the nonconsensual posting of someone's nude images online.[151] Federal bills to ban nonconsensual disclosure of intimate images have strong bipartisan support. Civil rights laws should be enforced against stalkers who interfere with victims' employment opportunities because they belong to traditionally subordinated groups.[152]

What about platforms that host online assaults? Some platforms solicit abuse yet still they can argue, quite correctly, that they enjoy immunity from liability under Section 230 of the Communications Decency Act. As one of

146. RICHARDS, INTELLECTUAL PRIVACY, *supra* note 10, at 107.

147 Danielle Keats Citron, *A Poor Mother's Right to Privacy*, 98 B.U. L. Rev. (forthcoming).

148. Citron, *Cyber Civil Rights*, *supra* note 8, at 86.

149 K&L Gates partners Elisa D'Amico and David Bateman are the leaders of this ground-breaking effort.

150. CITRON, HATE CRIMES, *supra* note 8, at 123.

151. *38 States + DC Have Revenge Porn Laws*, CYBER C.R. INITIATIVE https://www.cybercivil rights.org/ revenge-porn-laws/ (last visited Mar. 10, 2018).

152. CITRON, HATE CRIMES, *supra* note 8, at 158.

us (Citron) and Benjamin Wittes have argued, the time has come to revisit section 230's immunity provision.[153] Section 230 was meant to encourage self-monitoring from parties in the best position to efficiently prevent harm to third parties.[154] It was meant to immunize platforms from liability related to under- and over-filtering of "offensive" material.[155] The problem is that an overbroad interpretation of Section 230 enables the exercise of great power with no concomitant responsibility.[156] Sites not only can deliberately ignore reports of abuse, but they also can encourage and solicit abuse and still enjoy the shelter of section 230's immunity provision.[157] Federal lawmakers should revise Section 230 to condition the immunity on reasonable efforts to address known illegality.[158]

Third, the promise of technology must be available to all and not thwarted by a deepening of the so-called "digital divide." The economic, expressive, and other opportunities enabled by digital technologies will be limited at best if only the privileged can enjoy them. This is a reality that even Silicon Valley recognizes.[159] However, despite the broad recognition of the problem of the digital divide, it remains under-theorized and under-addressed in the legal literature.

In privacy scholarship, two influential books have examined the sociology of how poverty impacts privacy rights. In *Overseers of the Poor*, John Gilliom explored how the welfare system deprives recipients of any privacy agency.[160] In *The Poverty of Privacy Rights*, Khiara Bridges powerfully demonstrated that poor mothers are subject to invasive, persistent state surveillance, whether or not they receive public funding for prenatal care, at great cost to their self-worth and equal standing as citizens.[161] These works demonstrate how the state uses its provision of

153. *See* Citron & Wittes, *supra* note 120; *see also* Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, GEO. L. TECH. REV. (forthcoming 2018) (on file with authors); Danielle Keats Citron, Section 230's Challenge to Civil Rights and Civil Liberties, Knight First Amendment Institute at Columbia University, https://knightcolumbia.org/content/section-230s-challenge-civil-rights-and-civil-liberties. For a compelling argument that section 230 is due for an overhaul to ensure platform responsibility for discriminatory designs and other civil rights violations, see Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 1 (forthcoming 2018).

154. Citron & Wittes, *supra* note 120, at 405–06.

155. *Id.* at 406.

156. *See generally* Tushnet, *supra* note 125.

157. Citron & Wittes, *supra* note 120, at 413–14.

158. *Id.* at 419.

159. *E.g.*, ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS (2013) (acknowledging the importance of the "digital divide").

160. JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY (2001); *see also* Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163 (2003) (relating Gilliom's work to the legal literature of privacy).

161. KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017); *see also* Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. (forthcoming 2018).

public benefits and concern about child welfare to deprive individuals of meaningful privacy protections.

In the context of platforms and free expression, however, the literature is underdeveloped. This has likely been the case because in the American legal academy, "free expression" has for decades meant the First Amendment; the vast body of constitutional doctrine has certainly provided a fertile ground for scholarly analysis. However, one unfortunate consequence has been that most legal academics have focused on judicial doctrines of equality of treatment for expression rather than on the practical matter of equality of access to expressive channels.[162] Although few exceptions in the literature exist, the single-minded focus on legal doctrine rather than the actual ability to access the Internet means that we lack a basic vocabulary to talk about power and inequality in the realm of free expression when the state is not involved. For law to enable free expression in the new digital expressive environment, we must ensure that the access to that environment is not limited to the privileged few, and that we have the words, models, and examples to talk about these problems critically and constructively.

### *C. Structure Matters*

Beyond inputs, we need to pay attention to the social, economic, and technical structures that facilitate digital expression. This requires us to focus on the structure of what Thomas Emerson helpfully called our "system of free expression."[163] Legal rules and policies affecting free expression must take into account the structures upon which they operate. Legal rules do not operate in a vacuum, and different rules will operate differently in different structures.

The design of policies to promote digital expression must take into account the structures of free speech in a digital age. Two factors are particularly important in designing these rules. First, our rules must be suitable for the level of the stack we are talking about. Second, we must ensure, either via network neutrality concepts or other basic rules of fairness, that private gatekeepers cannot be permitted to unreasonably throttle, block, or censor expression.

When thinking about the structure of our system of free expression, we must first consider the context in which a rule operates, as well as its relationship to the system as a whole. Consider again the "stack" metaphor's conception of the Internet as involving the backbone as the bottom (or

162. There are a few exceptions. *See, e.g.*, Marvin Ammori, *First Amendment Architecture*, 2012 WIS. L. REV. 1, 50–53; Balkin, *Cultural Democracy and the First Amendment*, *supra* note 32.

163. THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION (1970).

essential foundation) and applications and content as higher up in a "stack" of technical and social processes. Companies operating at different layers of the stack have varying degree of power over digital expression. That power differential should be central to a legal regime designed to protect against private companies' power over expression in the digital age. Rules that make sense for Internet service providers, where there are few alternatives and limited (or no) competition in the market and where control over access to the Internet can be total, might make no sense for content platforms, where there is considerable market competition and alternative outlets for speech.

In assessing the power differentials of different layers of the stack, lawmakers must avoid falling under the spell of new technologies and the magical thinking that they inevitably inspire. New technologies are often viewed as inherently valuable. The tendency is to credit (and even to fetishize) a new technology's potential upsides and discredit its possible downsides. Big Data, for instance, is often billed as the "New Oil."[164] Blinded by arguments concerning trade secrets and social utility, legislatures and courts have yet to reckon with the negative externalities wrought by the scoring, ranking, and rating of individuals enabled by Big Data.[165] Furthermore, many judges and commentators fail to appreciate the complexity of the Internet, the nuances of the stack, or the critical technological and social contexts that operate differently at its different levels.

The Supreme Court in *Packingham* fell into precisely these traps of reductionism andmagical thinking.The Court left some room for nuance, however. At the outset, the Court acknowledged that the digital revolution is wide-ranging, and that judges should tread carefully lest they rule broadly in ways that create problems for the law in the future. It explained that:

> While we now may be coming to the realization that the Cyber Age is a revolution of historic proportions, we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be. The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete

164. For a critical exploration of this commonly invoked concept, see Dennis D. Hirsch & Jonathan H. King, *Big Data Sustainability: An Environmental Management Systems Analogy*, 72 WASH. & LEE L. REV. ONLINE 406, 408 (2016).

165. *See generally* Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41 (2013); Neil M. Richards & Jonathan H. King, *Big Data and the Future for Privacy*, *in* RESEARCH HANDBOOK ON DIGITAL TRANSFORMATIONS 272 (F. Xavier Olleros & Majlinda Zhegu eds., 2016); Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393 (2014).

tomorrow.[166]

On the other hand, as Justice Alito pointed out astutely in his concurring opinion (in which he was joined by the Chief Justice and Justice Thomas): "It is regrettable that the Court has not heeded its own admonition of caution."[167] By treating the Internet and cyberspace in a unitary way, the Court suggested that all of cyberspace (or at least its "vast democratic forums") amounted to a public forum subject to the full force of the First Amendment, a suggestion that, if taken seriously, could make it needlessly difficult for legislatures to deal with real problems of crime, abuse, stalking, hacking, harassment, and fraud in digital contexts.

How courts talk about the Internet matters, not only in how they decide individual cases, but also in how they frame similar issues for future courts. Unfortunately, in *Packingham*, the Court conflated the Internet and social media as meaning essentially the same thing. Then too, the Court said that different content platforms were the same—Facebook is interchangeable with LinkedIn and Twitter, in other words. In so doing, the Court ignored the importance of context, and in particular failed to recognize the crucial differences in the different layers of the stack, let alone the different affordances (and limits) of the various content platforms.

*Packingham* dealt with an unreasonably overbroad government rule that interfered with sex offenders' ability to access the Internet and engage in the social processes of free expression. But as we have explained, government power is not the only kind of power that can affect our ability to express ourselves using digital tools. The private gatekeepers that exercise control over the Internet's expressive infrastructure exercise substantial power over opportunities to speak, engage, interact, and associate freely. We must be careful to ensure that this power is also checked in the interests of promoting free expression. Here too, law has a role to play, in making sure that these gatekeepers cannot unreasonably throttle or censor the expression of others, through commitments to network neutrality and other basic rules of fairness.

A systematic exploration of the potential regulatory regimes for the varying stacks of the Internet is a project for another day. For now, we note a few rules of thumb. Private power over digital expression should be paired with responsibility to the public. As a company's power over digital expression grows closer to total (meaning there are few to no alternatives to express oneself online), the greater the responsibilities (via regulation)

166. Packingham v. North Carolina, 137 S. Ct. 1730, 1736.
167. *Id.* at 1744 (Alito, J., concurring).

attendant to that power. When companies wield power over speech that is akin to state power, regulation should be tailored to reflect that power.

Consider public utilities. In the industrial age, public utility regulation emerged to address private power over essential infrastructure, such as railroads and telephones. In the information age, the backbone layer of the Internet stack wields similar influence over our political economy. That includes broadband providers that are already considered common carriers under Title II of the Communications Act of 1934. But it should also include Internet service providers that determine whether one has any online access in some locations. The same might be said of security services like Cloudflare that have the power to wipe a site off the Internet.[168]

### *D. Values Matter*

If we are to craft laws and policies that promote meaningful digital free expression, we have argued, we must avoid magical thinking and be attentive to the inputs and structure of our expressive infrastructure. Laws and policies affecting digital expression cannot be merely neutral or narrowly procedural; they must be substantive, which is to say that we must do our best to ensure that the values of the First Amendment are faithfully translated to the digital environment. This means that we must steer the difficult course between recognizing that the digital environment has features that are different from the mass media and physical world of the twentieth century, while remaining immune from the romantic lure and magical thinking of Internet exceptionalism.

We must also ensure that the First Amendment continues to apply in digital formats but not be seduced by overbroad readings of the First Amendment. In our opinion, the *Reno* and *Packingham* cases came out the right way: they correctly invalidated clumsy attempts by legislatures that were either intended to force digital expression into a particular anodyne direction (*Reno*) or designed to deal with a real problem in a way that was highly overbroad (*Packingham*). But easy cases can make bad law too. Each case reached the correct result but on the basis of a flawed and unrealistic view of the Internet as it actually operates, a view that could cause mischief not only in other court cases, but also in legislative and agency decision-making regarding digital speech. Put simply, how we talk about the Internet matters, and theory matters.

168. Speaking with regret about his decision to drop the Daily Stormer as a client, Cloudflare's CEO Matthew Prince said, "I think the people who run The Daily Stormer are abhorrent. But again I don't think my political decisions should determine who should and shouldn't be on the internet." Kate Conger, *Cloudflare CEO on Terminating Service to Neo-Nazi Site: 'The Daily Stormer Are Assholes*,' GIZMODO (Aug. 16, 2017, 6:00 PM), https://perma.cc/RD9N-ZUEB.

Beyond the First Amendment's foundational commitment to debate on public matters that is uninhibited, robust, and wide-open, we believe that any theory animating legal rules to protect free speech in the digital age should keep a number of core principles in mind. Fundamentally, we must faithfully translate the principles of our analog twentieth century to the digital twenty-first century. Part of this process will be the traditional processes of translation that have been discussed in the legal literature since Joel Reidenberg's and Lawrence Lessig's pioneering work in the 1990s.[169] In this respect, the translation to digital formats of hard-won, expressive liberties against the state will remain as important as the translation of other fundamental rights, such as the Fourth Amendment's protection of privacy.[170] But just as digital privacy rights require protection against both public and private actors, so does the right to free expression. Even when the First Amendment is properly translated to the digital context, we need to make sure that its values are advanced against private power in digital environments where the state action doctrine renders constitutional doctrine inapplicable. If we are committed to ensuring that our expressive traditions survive the translation to the digital age, nurturing the capacity of free speech in privately-controlled online environments will be essential.

No doubt, this part of the project will be challenging. Whereas the Anglo-American legal tradition has a vocabulary and legal regime for dealing with government power dating back centuries, if not to the Magna Carta itself, our tradition is much less developed with respect to private power. Because we lack an agreed-upon vocabulary to deal with private acts of censorship, developing legal tools to deal with that problem will be challenging. Nevertheless, it is a challenge we must take up if we want to ensure that our hard-won commitment to expressive liberties in the twentieth century survives the twenty-first.

## CONCLUSION

In *Packingham*, the Court explained that the "the Cyber Age is a revolution of historic proportions" whose "full dimensions and vast potential to alter how we think, express ourselves, and define who we want

169. *See* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE (1999).

170. *See* Neil M. Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441 (2018); Neil M. Richards, *Secret Government Searches and Digital Civil Liberties*, *in* A TWENTY-FIRST CENTURY FRAMEWORK FOR DIGITAL PRIVACY (Nat'l Constitution Ctr. 2017), https://constitution center.org/ digital-privacy.

to be" have not been fully realized.[171] It warned that the Internet's positive potential was "so new, so protean, and so far reaching."[172] On the other hand, criminal downsides to the Internet were merely hypothetical.[173] Although the costs of cyberstalking, impersonation, and identity theft (to name just a few) were already well documented, the majority described the Internet as a new technology that had not yet been exploited for criminal ends: "For centuries now, inventions heralded as advances in human progress have been exploited by the criminal mind. New technologies, *all too soon*, can become instruments used to commit serious crimes. The railroad is one example, and the telephone another. So, it will be with the Internet and social media."[174]

In one important sense, the Court's analysis in *Packingham* hit the nail on the head entirely. Although its "Cyber Age" rhetoric seems a bit dated, the Court is exactly correct that the digital revolution is radically reshaping how we think, read, and communicate. The effects of this transformation on our expressive culture, arts, and politics cannot be fully understood while we are in the midst of such rapid and ever-morphing change. It is important, as the Court suggested, to move cautiously and with intellectual and epistemic modesty as we try to chart a course to ensure our commitments to free speech adapt to changing social and technological circumstances.

But as this article has explained, in another more fundamental sense, the Supreme Court's analysis in *Packingham* was woefully misguided. Whether we call it the digital revolution or "the Cyber Age," it is essential that we take our networked society as it is rather than we (or the marketing departments of technology companies) would like it to be. In thinking about how to protect free speech and other civil liberties in digital environments, we must remain modest, but we must also be realistic about the costs and the challenges posed by our largely privately-owned expressive infrastructure. At the same time that we are translating our free speech protections to our rapidly changing digital contexts, we need to be wary of the problem of private power, so that our new system of free expression is crafted to deal with the real challenges it faces, rather than ones it fails to consider.

This is a real challenge, and whether and how we respond to it will be one of the defining legacies of our time. At stake is nothing less than self-government itself. As we move cautiously but realistically into our digital brave new world, we should keep in mind the four principles we have outlined in this article—the avoidance of magical thinking, the importance

171. *Packingham*, 137 S. Ct. at 1736.
172. *Id.*
173. *Id.*
174. *Id.* (emphasis added) (citations omitted).

of inputs and structure, and the need to remain true to the values that have animated our First Amendment tradition, when dealing with private power in addition to that of the state. Other principles will inevitably be needed, but these four are a good place to start.